

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Critical GoAnywhere MFT Flaw Allows Attackers to Become Admins**

Date of Publication

January 25, 2024

Admiralty Code

A1

TA Number

TA2024032




# Summary

**First Seen:** December 4, 2023

**Affected Platform:** Fortra GoAnywhere MFT

**Impact:** A critical authentication bypass vulnerability (CVE-2024-0204) in Fortra GoAnywhere MFT enables attackers to create new admin users with full privileges, potentially leading to data exfiltration, malware deployment, and further attacks within the network.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-0204	Fortra GoAnywhere MFT Authentication bypass Vulnerability	Fortra GoAnywhere MFT			

# Vulnerability Details

## #1

A critical vulnerability in Fortra GoAnywhere MFT, tracked as CVE-2024-0204, allows attackers to create a new admin user through the administration portal without requiring valid credentials. Proof-of-Concept (PoC) exploit code for this critical vulnerability has been released, raising concerns about potential exploitation by attackers. The vulnerability affects versions 6.x from 6.0.1 and versions 7.x before 7.4.1, with a fix released in version 7.4.1 on December 7, 2023.

## #2

While Fortra issued an advisory urging customers to upgrade, there are still over 3,000 internet-exposed Fortra GoAnywhere MFT admin portals, according to the Shodan search engine. The CIOP ransomware gang had previously exploited a zero-day vulnerability ([CVE-2023-0669](#)) in the same solution in early 2023.

# Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-0204	Fortra GoAnywhere MFT 6.x from 6.0.1 Fortra GoAnywhere MFT 7.x before 7.4.1	cpe:2.3:a:fortra:goanywh ere_mft:*:*:*:*:*	CWE-425

## Recommendations



**Immediate Upgrade:** Organizations using Fortra GoAnywhere MFT should promptly upgrade their installations to version 7.4.1 or higher, where the CVE-2024-0204 vulnerability has been addressed. This is the most effective measure to mitigate the risk of exploitation.



**Restrict Service Access:** If upgrading is not immediately possible, consider limiting exposure of Fortra GoAnywhere MFT admin portals. This can be achieved by creating access rules to whitelist specific network addresses and, at a minimum, removing the admin portal from the public internet.



**Monitor Admin Users Group:** Regularly monitor the Admin Users group in the GoAnywhere administrator portal, specifically in the Users -> Admin Users section. Look for any unauthorized additions to the Admin Users group, which could indicate a compromise.



**Network Monitoring:** Implement comprehensive network monitoring to detect and respond to any unusual or suspicious activities. Pay special attention to unexpected access patterns or connections, as these may indicate attempted exploits.

## Potential MITRE ATT&CK TTPs

<b><u>TA0002</u></b> Execution	<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0005</u></b> Defense Evasion
<b><u>TA0004</u></b> Privilege Escalation	<b><u>T1588.005</u></b> Exploits	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1211</u></b> Exploitation for Defense Evasion
<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1556</u></b> Modify Authentication Process

## Patch Details

Upgrade Fortra GoAnywhere MFT to version 7.4.1 or later versions.

Workaround:

To mitigate the vulnerability in non-container deployments, delete "InitialAccountSetup.xhtml" and restart services. For container deployments, replace the file with an empty one and secure the container environment against unauthorized access.

Link:

<https://www.fortra.com/security/advisory/fi-2024-001>

## References

<https://www.horizon3.ai/cve-2024-0204-fortra-goanywhere-mft-authentication-bypass-deep-dive/>

[https://beta.shodan.io/search?query/html:"InvalidBrowser.xhtml](https://beta.shodan.io/search?query/html:)

<https://packetstormsecurity.com/files/related/176683/GoAnywhere-MFT-Authentication-Bypass.html>

<https://github.com/horizon3ai/CVE-2024-0204>

<https://www.hivepro.com/clop-ransomware-group-claims-responsibility-for-goanywhere-mft-attacks/>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**January 25, 2024 • 2:30 AM**

© 2024 All Rights are Reserved by Hive Pro<sup>®</sup>



More at [www.hivepro.com](http://www.hivepro.com)